



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/014,873	12/14/2001	Jonathan Edwards	19903.0012	1763

23517 7590 01/12/2006

SWIDLER BERLIN LLP  
3000 K STREET, NW  
BOX IP  
WASHINGTON, DC 20007

EXAMINER

ZAND, KAMBIZ

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 01/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 10/014,873	<b>Applicant(s)</b> EDWARDS ET AL.	
	<b>Examiner</b> Kambiz Zand	<b>Art Unit</b> 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 22 November 2005.  
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.  
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-48 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
6) ☒ Claim(s) 1-2, 4-15, 17-28, 30-41 and 43-48 is/are rejected.  
7) ☒ Claim(s) 3, 16, 29 and 42 is/are objected to.  
8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.  
10) ☒ The drawing(s) filed on 14 December 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

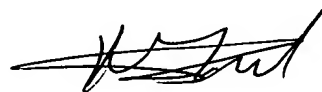
#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)  
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)  
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.  
4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.  
5) ☐ Notice of Informal Patent Application (PTO-152)  
6) ☐ Other: \_\_\_\_\_.



### **DETAILED ACTION**

1. The text of those sections of Title 35, U.S. Code not included in this section can be found in the prior office action.
2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
3. Claims 1, 7, 14, 20, 27 and 33 have been amended.
4. New claims 40-48 have been added.
5. Claims 1-48 are pending.

### ***Response to Arguments***

6. Applicant's arguments with respect to the claims have been considered but are moot in view of the new ground(s) of rejection.
- In response to applicant's arguments, the time interval between the interception and the scanning is taught by Le Pennec where files are intercepted in real time and after the interception it is scanned or where the file after interception are compared with stored files to check if the signature is different in order to issue the scanning in case of the difference checksum, such time after the interception and before the scanning corresponds to applicant's "waiting time" (see page 1-2.
  - However Examiner has given weight to applicant's arguments in view of claims 3, 16, 29 and 42 where if such limitation taken into account then the applicant's

arguments are persuasive. Therefore the rejections of claims 3, 16, 29 and 42 have been withdrawn (please see allowable subject matters below).

***Claim Rejections - 35 USC § 102***

7. **Claims 1-2, 4-15, 17-28, 30-41 and 43-48** are rejected under 35 U.S.C. 102(e) as being anticipated by Le Pennec et al (2001/0020272 A1).

**As per claims 1, 14 and 27** Le Pennec et al (2001/0020272 A1) teach a method, system and computer program product of detecting a malware comprising the steps of: monitoring file access operations of a process (see page 2); intercepting a file access operation of the process to a file (see page 2, paragraph 0042 and 0043); in response to the intercepting, waiting a time interval between the intercepting and scanning the file for a malware (see page 2, paragraph 0046-0050); and scanning the file for the malware, after waiting the time interval (see page 2, paragraph 0046-0050).

**As per claims 2, 15 and 28** Le Pennec et al (2001/0020272 A1) teach the method, system and computer program product of claims 1, 14 and 27, wherein the process is associated with an application program (see page 2-16 where many instances relates to the above limitation).

**As per claims 4, 17 and 30** Le Pennec et al (2001/0020272 A1) teach the method, system and computer program product of claims 1, 14 and 27, wherein the file has a specified file type (see page 2-16 where many instances relates to the above limitation).

**As per claims 5, 18 and 31** Le Pennec et al (2001/0020272 A1) teach the method, system and computer program product of claims 1, 14 and 27, wherein the time interval is predefined (see page 2, paragraph 0046-0050).

**As per claims 6, 19 and 32** Le Pennec et al (2001/0020272 A1) teach the method, system and computer program product of claims 1, 14 and 27, wherein the time interval is user-defined (see page 2 where setting the manual time interval is considered as user defined time interval).

**As per claims 7, 20 and 33** Le Pennec et al (2001/0020272 A1) teach the method, system and computer program product of claims 1, 14 and 27, wherein the time interval is based on a file type of the file (see page 2-16 where many instances relates to the above limitation).

**As per claims 8, 21 and 34** Le Pennec et al (2001/0020272 A1) teach the method, system and computer program product of claims 1, 14 and 27, wherein the time interval

Art Unit: 2132

is based on the process(see page 2-16 where many instances relates to the above limitation).

**As per claims 9, 22 and 35** Le Pennec et al (2001/0020272 A1) teach the method, system and computer program product of claims 1, 14 and 27, wherein the malware is a computer virus (see page 2).

**As per claims 10, 23 and 36** Le Pennec et al (2001/0020272 A1) teach the method, system and computer program product of claims 1, 14 and 27, wherein the malware is a computer worm (see page 2-5).

**As per claims 11, 24 and 37** Le Pennec et al (2001/0020272 A1) teach the method, system and computer program product of claims 1, 14 and 27, wherein the malware is a Trojan horse program.

**As per claims 12, 25 and 38** Le Pennec et al (2001/0020272 A1) teach the method, system and computer program product of claims 1, 14 and 27, further comprising the step of: allowing the intercepted file access operation of the process to a file to complete ((see page 2-16 where many instances relates to the above limitation).

**As per claims 12, 26 and 39** Le Pennec et al (2001/0020272 A1) teach the method, system and computer program product of claims 12, 54 and 38, further comprising the

Art Unit: 2132

step of: allowing at least one additional file access operation of the process to a file that occurs before the scanning of the file for a malware to complete (see page 2-16 where many instances relates to the above limitation).

**As per claim 40** Le Pennec et al (2001/0020272 A1) teach the method of claim 1, wherein at least a portion of the file access operations are completed before the scanning (see page 2-16).

**As per claim 41** Le Pennec et al (2001/0020272 A1) teach the method of claim 1, wherein at least a portion of the file access operations are completed during the scanning (see page 2-16).

**As per claim 43** Le Pennec et al (2001/0020272 A1) teach the method of claim 1, wherein the file access operations that occur on the file after the intercepting of a file write operation are completed during the scanning (see page 2-16).

**As per claim 44** Le Pennec et al (2001/0020272 A1) teach the method of claim 1, wherein the file access operations lasts less than the time interval, only a last file access operation of the set is scanned (see page 2-16).

**As per claim 45** Le Pennec et al (2001/0020272 A1) teach the method of claim 1, wherein only a sample of a set of the file access operations is scanned (see page 2-16).

**As per claim 46** Le Pennec et al (2001/0020272 A1) teach the method of claim 1, wherein a final version of the file is scanned, after all of the file access operations of a set are complete (see page 2-16).

**As per claim 47** Le Pennec et al (2001/0020272 A1) teach the method of claim 1, wherein the time interval is longer than at least one of an open cycle, a write cycle, and a close cycle associated with the file access operations (see page 2-16).

**As per claim 48** Le Pennec et al (2001/0020272 A1) teach the method of claim 1, wherein the time interval is initiated after interception of a first file access operation such that, during the time interval, multiple subsequent file access operations are completed without the scanning, after which the file is scanned (see page 2-16).

### ***Allowable Subject Matter***

8. **Claims 3, 16, 29 and 42** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

### **Conclusion**



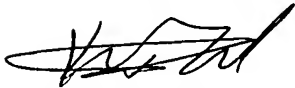
9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (571) 272-3811. The examiner can normally be reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone numbers for the organization where this application or proceeding is assigned are 571-272-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR

Art Unit: 2132

or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Kambiz Zand

01/03/2006

AU2132